EKI-6311GN

IEEE 802.11 b/g/n Wireless
Access Point/Client Bridge

User Manual

Copyright

The documentation and the software included with this product are copyrighted 2010 by Advantech Co., Ltd. All rights are reserved. Advantech Co., Ltd. reserves the right to make improvements in the products described in this manual at any time without notice. No part of this manual may be reproduced, copied, translated or transmitted in any form or by any means without the prior written permission of Advantech Co., Ltd. Information provided in this manual is intended to be accurate and reliable. However, Advantech Co., Ltd. assumes no responsibility for its use, nor for any infringements of the rights of third parties, which may result from its use.

Acknowledgements

Intel and Pentium are trademarks of Intel Corporation.
Microsoft Windows and MS-DOS are registered trademarks of Microsoft Corp.
All other product names or trademarks are properties of their respective owners.

Product Warranty (2 years)

Advantech warrants to you, the original purchaser, that each of its products will be free from defects in materials and workmanship for two years from the date of purchase.

This warranty does not apply to any products which have been repaired or altered by persons other than repair personnel authorized by Advantech, or which have been subject to misuse, abuse, accident or improper installation. Advantech assumes no liability under the terms of this warranty as a consequence of such events.

Because of Advantech's high quality-control standards and rigorous testing, most of our customers never need to use our repair service. If an Advantech product is defective, it will be repaired or replaced at no charge during the warranty period. For out-of-warranty repairs, you will be billed according to the cost of replacement materials, service time and freight. Please consult your dealer for more details.

If you think you have a defective product, follow these steps:

1. Collect all the information about the problem encountered. (For example, CPU speed, Advantech products used other hardware and software used, etc.) Note anything abnormal and list any onscreen messages you get when the problem occurs.
2. Call your dealer and describe the problem. Please have your manual, product, and any helpful information readily available.
3. If your product is diagnosed as defective, obtain an RMA (return merchandize authorization) number from your dealer. This allows us to process your return more quickly.
4. Carefully pack the defective product, a fully-completed Repair and Replacement Order Card and a photocopy proof of purchase date (such as your sales receipt) in a shippable container. A product returned without proof of the purchase date is not eligible for warranty service.
5. Write the RMA number visibly on the outside of the package and ship it prepaid to your dealer.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. To avoid the possibility of exceeding radio frequency exposure limits, you shall beep a distance of at least 100cm between you and the antenna of the installed equipment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Technical Support and Assistance

Step 1. Visit the Advantech web site at **www.advantech.com/support** where you can find the latest information about the product.

Step 2. Contact your distributor, sales representative, or Advantech's customer service center for technical support if you need additional assistance. Please have the following information ready before you call:
- Product name and serial number
- Description of your peripheral attachments
- Description of your software (operating system, version, application software, etc.)
- A complete description of the problem
- The exact wording of any error messages

Safety Instructions

1. Read these safety instructions carefully.
2. Keep this User's Manual for later reference.
3. Disconnect this equipment from any AC outlet before cleaning. Use a damp cloth. Do not use liquid or spray detergents for cleaning.
4. For plug-in equipment, the power outlet socket must be located near the equipment and must be easily accessible.
5. Keep this equipment away from humidity.
6. Put this equipment on a reliable surface during installation. Dropping it or letting it fall may cause damage.
7. The openings on the enclosure are for air convection. Protect the equipment from overheating. DO NOT COVER THE OPENINGS.
8. Make sure the voltage of the power source is correct before connecting the equipment to the power outlet.
9. Position the power cord so that people cannot step on it. Do not place anything over the power cord.
10. All cautions and warnings on the equipment should be noted.
11. If the equipment is not used for a long time, disconnect it from the power source to avoid damage by transient over voltage.
12. Never pour any liquid into an opening. This may cause fire or electrical shock.
13. Never open the equipment. For safety reasons, the equipment should be opened only by qualified service personnel.
14. If one of the following situations arises, get the equipment checked by service personnel:
    a. The power cord or plug is damaged.
    b. Liquid has penetrated into the equipment.
    c. The equipment has been exposed to moisture.
    d. The equipment does not work well, or you cannot get it to work according to the user's manual.
    e. The equipment has been dropped and damaged.
    f. The equipment has obvious signs of breakage.

15. DO NOT LEAVE THIS EQUIPMENT IN AN ENVIRONMENT WHERE THE STORAGE TEMPERATURE MAY GO BELOW -40℃ (-40℉) OR ABOVE 85℃ (185℉). THIS COULD DAMAGE THE EQUIPMENT. THE EQUIPMENT SHOULD BE IN A CONTROLLED ENVIRONMENT.

Safety Precaution - Static Electricity

Follow these simple precautions to protect yourself from harm and the products from damage.

1. To avoid electrical shock, always disconnect the power from your PC chassis before you work on it. Don't touch any components on the CPU card or other cards while the PC is on.
2. Disconnect power before making any configuration changes. The sudden rush of power as you connect a jumper or install a card may damage sensitive electronic components.

Contents

CHAPTER 1 OVERVIEW 3

1.1 Introduction 3
1.2 Features 3
1.3 Specification 4
1.4 Packing List 5
1.5 Safety Precaution 6

CHAPTER 2 INSTALLATION 8

2.1 Preparation before Installation 8
2.2 Installation Precautions 9
2.3 Hardware Installation 9
2.4 Pole Mounting 12

CHAPTER 3 BASIC SETTINGS 16

3.1 Factory Default Settings 16
3.2 System Requirements 16
3.3 How to Login the Web-based Interface 17
3.4 Basic System Settings 18
3.5 RADIUS Settings 20
3.6 Time Settings 21
3.7 Firewall Settings 22
3.8 Basic Wireless Settings 25
3.9 Site Survey 27

CHAPTER 4 ADVANCED SETTINGS 29

4.1 Advanced Wireless Settings 29
4.2 Wireless Security Settings 31
4.3 Access Control 32
4.4 WDS Settings 33

CHAPTER 5 MANAGEMENT 35

5.1 SNMP Management 35
5.2 Password 37
5.3 Backup/ Retrieve Settings 39
5.4 Restore Factory Default Settings 40
5.5 Reboot 40
5.6 System Log 41
5.7 Site Survey 41
5.8 Ping Watch Dog 42

CHAPTER 6 STATUS 44

6.1 View EKI-6311GN Basic Information 44
6.2 View Association List 44
6.3 View Network Flow Statistics 46
6.4 View Bridge Table 46
6.5 View ARP Table 47
6.6 View Active DHCP Client Table 47

CHAPTER 7 TROUBLE SHOOTING 49

CHAPTER 1

Overview

Chapter 1 Overview

1.1 Introduction

EKI-6311GN is a feature rich wireless AP/ CPE which provides a reliable wireless connectivity for industrial environments. The PoE injector enhances flexibility in deployment of this AP/ CPE even where the DC power supply is hard to fulfill. As an 802.11n compliant device, EKI-6311GN provides 3 times higher data rates than legacy 802.11g devices. With the support of STP, WMM and IGMP snooping protocols, EKI-6311GN effectively improves the reliability of wireless connectivity, especially in applications that need high reliability and high throughput data transmission. To secure wireless connections, EKI-6311GN encrypts data through 64/128/152-bit WEP data encryption and also supports WPA2/WPA/802.1x for powerful security authentication.

1.2 Features

- Compliant with IEEE 802.11b/g and IEEE 802.11n draft 2.0
- Support Power-through-Ethernet which is supplied with 12V.
- High reliable water-tight housing endures almost any harsh environments
- Four operating modes including AP, Wireless Client, WDS and AP Repeater
- Support 64/128/152-bit WEP and 802.1X, WPA, WPA2, WPA&WPA2,WPA-PSK, WPA2-PSK, and WPA-PSK&WPA2-PSK etc
- User-friendly Web and SNMP-based management interface
- Embedded 8dBi directional antenna with external N-type connector for optional antenna
- High output power 600mW
- Support distances up to 5Km
- Spanning Tree and IGMP snooping protocol support



Figure 1 EKI-6311GN

1.3 Specification

Standard Support

- **Wireless** IEEE802.11b/g/n (IEEE802.11n draft v 2,0)
- **Ethernet** IEEE802.3u MDI / MDIX 10/100 Fast Ethernet
- **LAN** IEEE802.11b/g wireless LAN interface
  IEEE 802.11n draft wireless LAN standard
  Passive 12V PoE, max. distance: 50 meters
- **Certifications**
  US FCC Part 15 Class B & C & E
  Europe ETSI 300 328, ETSI 301 489-1&17
  EN 60950 compliant and CE Mark
- **Data Rates**
  802.11b 11, 5.5, 2, 1 Mbps, auto-fallback `
  802.11a/g 54, 48, 36, 24, 18, 12, 9, 6 Mbps, auto-fallback
  802.11n:
  6M, 6.5M, 13M, 13.5M, 19.5M, 26M, 27M, 39M,40.5M, 53M, 54M, 58.5M, 65M, 78M, 81M, 104M,108M, 117M, 121.5M, 130M, 135Mbps

Physical Specifications

- **Power** DC 12Volt / 1.0A; AC Adapter 100V~240V
- **Dimensions (L x W x H)** 228 x 64 x 61 mm
- **Weight** 500g

Interface Operation Modes

- Access Point (AP)
- Customer Premise Equipment (CPE)

Antenna

- **Antenna Configuration** 1x1 (1 Tx, 1 Rx)
- Default embedded 8dBi directional antenna (Vertical-Polarity)
- Reserve N-type Connector (Plug) *Switchable by software
- Equipped N-to-RSMA adaptor and 5dBi dipole antenna for indoor AP application.

Other Features

- Telnet, FTP, SNMP, Password Changes, Firmware updates, Configuration Files
- Radio on/off, WMM/Regatta Mode, Output Power Control, Fragmentation Length, Beacon Interval
- RTS/CTS threshold, DTIM Interval

Modulation Techniques

- **802.11b** DSSS (DBPSK, DQPSK, CCK)
- **802.11g** OFDM, DSSS (BPSK, QPSK, 16-QAM, 64-QAM)
- **802.11n** OFDM (BPSK, QPSK, 16-QAM, 64-QAM)

Channel Support

- **802.11b/g/ gn** HT20
  - FCC: CH1 ~ CH11; ETSI: CH1 ~ CH13
- **802.11gn** HT40
  - FCC: CH3 ~ CH9; ETSI: CH3 ~ CH11

Wireless Transmission Rates

- **Transmitted Power**
  - 802.11b: 26dBm802.
  - 11g: 26dBm @ 6Mbps, 24dBm @ 54Mbps802.
  - 11gn HT20: 26dBm @ MCS0, 22dBm@ MCS7802.
  - 11gn HT40: 26dBm @ MCS0, 21dBm@ MCS7

Receiver Sensitivity

- **802.11b Sensitivity** -93dBm @ 1Mbps; -88dBm @ 11Mbps
- **802.11g Sensitivity** -89dBm @ 6Mbps; -73dBm @ 54Mbps
- **802.11n HT20** -88dBm @ MCS0; -70dBm @ MCS7
- **802.11n HT40** -84dBm @ MCS0; -67dBm @ MCS7

1.4 Packing List

The product package you have received should contain the following items. If any of them are not included or damaged, please contact your local vendor for support.

EKI-6311GN	×1
Pole Mounting Ring	×1
Power Cord & PoE Injector	×1
Start up manual	×1
User's manual CD	×1
N-to-RSMA adaptor	×1
RSMA Omni antenna	×1

Pole Mounting Ring



Power Cord & PoE Injector

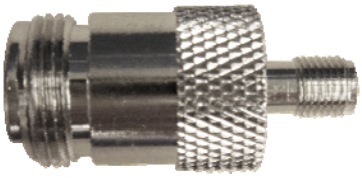


Start up manual & User's manual CD





N-to-RSMA adaptor



RSMA Omni Antenna



Figure 2 Accessories

Warning:

- Users MUST use the "Power cord & PoE Injector" shipped in the box with the EKI-6311GN. Use of other options will cause damage to the EKI-6311GN.

1.5 Safety Precaution

Attention *IF DC voltage is supplied by other power injector, please check the voltage and use a protection device on the power supply input.*

CHAPTER 2

Installation

Chapter 2 Installation

This chapter describes safety precautions and product information you have to know and check before installing EKI-6311GN.

2.1 Preparation before Installation

Professional Installation Required

Please seek assistance from a professional installer who is well trained in the RF installation and knowledgeable in the local regulations.

Safety Precautions

1. To keep you safe and install the hardware properly, please read and follow these safety precautions.
2. If you are installing EKI-6311GN for the first time, for your safety as well as others', please seek assistance from a professional installer who has received safety training on the hazards involved.
3. Keep safety as well as performance in mind when selecting your installation site, especially where there are electric power and phone lines.
4. When installing EKI-6311GN, please note the following things:
   - Do not use a metal ladder;
   - Do not work on a wet or windy day;
   - Wear shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.
5. When the system is operational, avoid standing directly in front of it. Strong RF fields are present when the transmitter is on.

2.2 Installation Precautions

To keep the EKI-6311GN well while you are installing it, please read and follow these installation precautions.

1. Users MUST use a proper and well-installed surge arrestor with the EKI-6311GN; otherwise, a random lightening could easily cause fatal damage to EKI-6311GN.

   EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRNTY.

2. Users MUST use the “Power cord & PoE Injector” shipped in the box with the EKI-6311GN. Use of other options will cause damage to the EKI-6311GN.
3. Users MUST power off the EKI-6311GN first before connecting the external antenna to it. Do not switch from built-in antenna to the external antenna from WEB management without physically attaching the external antenna onto the EKI-6311GN; otherwise, damage might be caused to the EKI-6311GN itself.

2.3 Hardware Installation

Connect up

1. The bottom of the EKI-6311GN is a movable cover. Grab the cover and pull it back harder to take it out as the figure shown below.

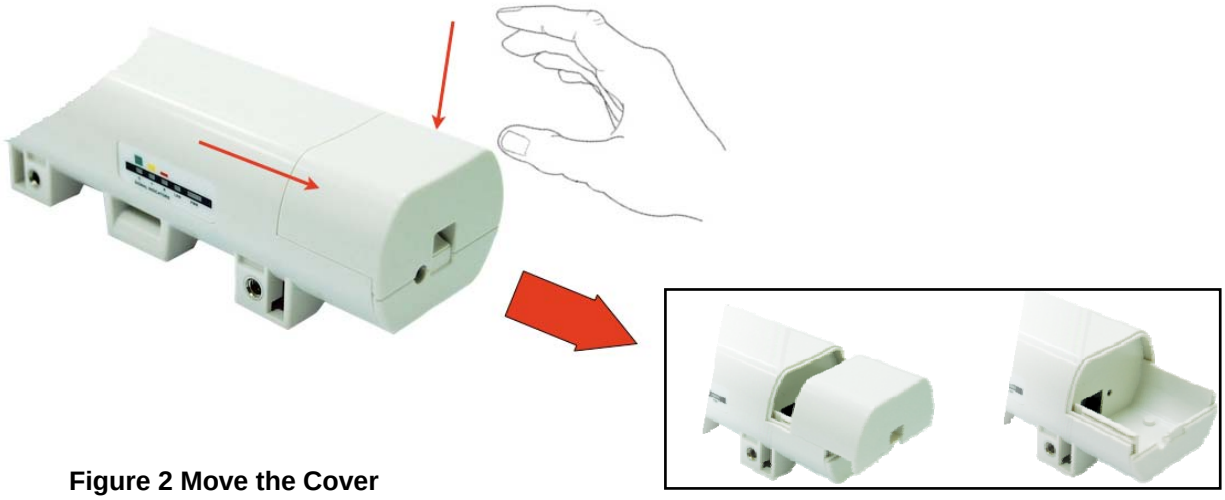


Figure 2 Move the Cover

2. Plug a standard Ethernet cable into the RJ45 port.



Figure 3 Cable Connection

3. Slide the cover back to seal the bottom of the EKI-6311GN.



Figure 4 Seal the Bottom

4. Plug the power cord into the DC port of the PoE injector as the following right picture shows.

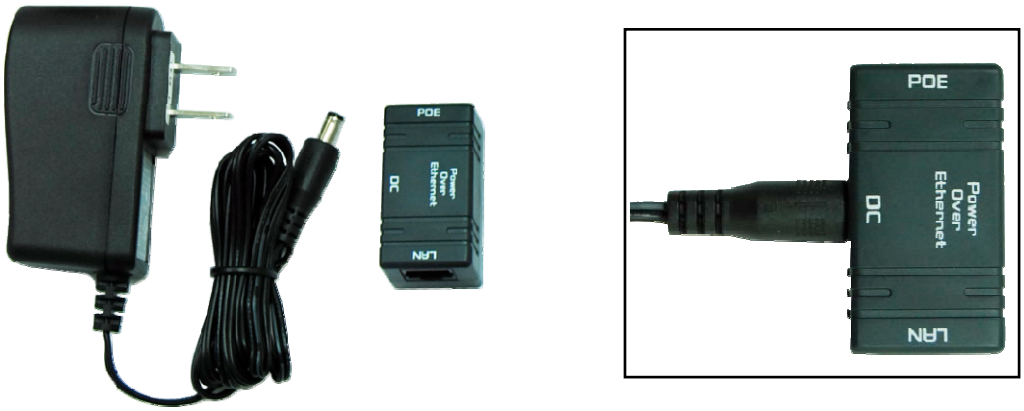


Figure 5 Connect to PoE Injector

5. Plug the other side of the Ethernet cable as shown in Step 3 into the PoE port of the PoE injector and get the complete set ready.



Figure 6 Complete Set

2.4 Pole Mounting

Pole Mounting

1. Turn the EKI-6311GN over. Put the pole mounting ring through the middle hole of it. Note that you should unlock the pole mounting ring with a screw driver before putting it through EKI-6311GN as the following right picture shows.

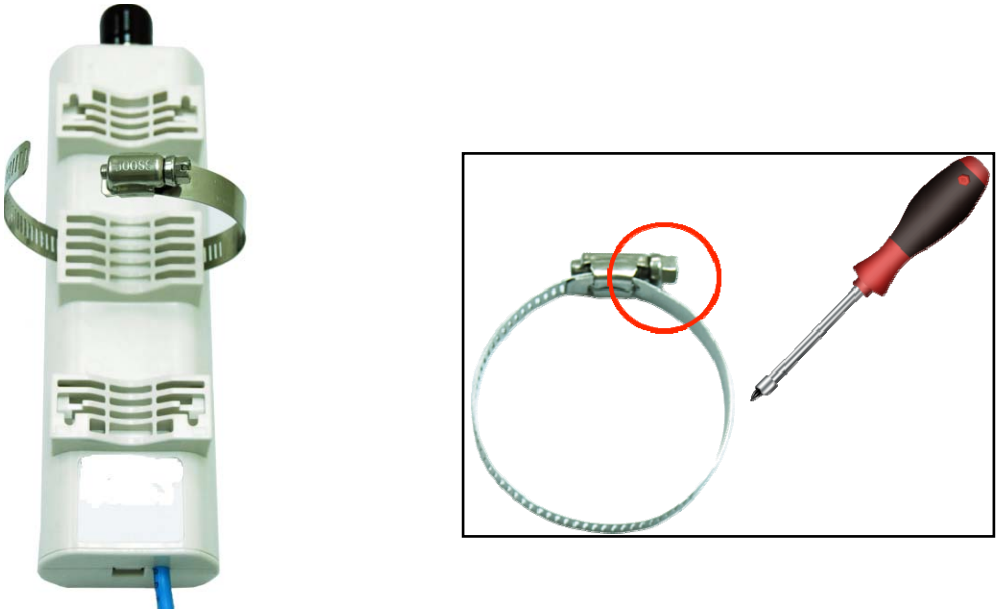


Figure 7 Pole Mounting – Step 1

2. Mount EKI-6311GN steadily to the pole by locking the pole mounting ring tightly.



Figure 8 Pole Mounting – Step 2

3. Now you have completed the hardware installation of EKI-6311GN.

Using the External Antenna

If you prefer to use the external antenna for your application instead of the built-in directional antenna, please follow the steps below.

1. Grab the black rubber on the top of EKI-6311GN, and slightly pull it up. The metal N-type connector will appear.

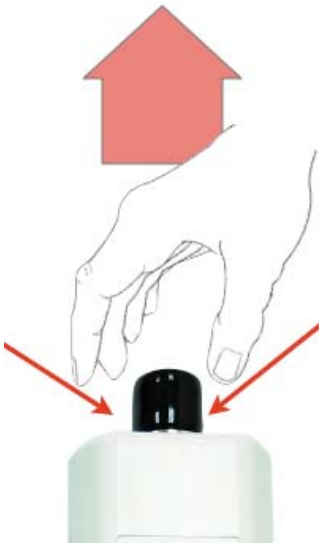


Figure 90 Move the Rubber

2. Connect your antenna with the N-type to RSMA adaptor on the top of EKI-6311GN. The following picture shows the full set of EKI-6311GN:



Figure 11 Removed the Rubber



Figure 12 Full set with antenna

Note:

- If you are going to use an external antenna on EKI-6311GN, get some cable in advance.
- Be aware of the force you use while connecting to the N-type connector, inappropriate force may damage the N-type connector!

Warning:

- Users MUST power off the EKI-6311GN first before connecting the external antenna to it. Do not switch from built-in antenna to the external antenna from WEB management without physically attaching the external antenna onto the EKI-6311GN; otherwise, damage might be caused to the EKI-6311GN itself.

CHAPTER 3

Basic Settings

Chapter 3 Basic Settings

3.1 Factory Default Settings

We'll elaborate the EKI-6311GN factory default settings. You can re-acquire these parameters by default. If necessary, please refer to the "Restore Factory Default Settings".

Table 1 EKI-6311GN Factory Default Settings

Features		Factory Default Settings
Username		admin
Password		password
Wireless Device Name		apXXXXXX (X represents the last 6 digits of Ethernet MAC address)
Operating Mode		AP
Data Rate		Auto
LAN	IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
	Gateway	0.0.0.0
	Primary DNS Server	0.0.0.0
	Secondary DNS Server	0.0.0.0
Spanning Tree		Enable
802.11 Mode		802.11b/g/n
Channel Number		6
SSID		Wireless
Broadcast SSID		Enable
HT Protect		Disable
Data Rate		Auto
Output Power		100% (Full)
Channel Mode		20MHz
WMM		Enabled
RTS Threshold (byte)		2346
Fragmentation Length (byte)		2346
Beacon Interval		100
DTIM Interval		1
Space in Meter		0
Flow Control by AP		Disable
Security		Open System
Encryption		None
Wireless Separation		Disable
Access Control		Disable
SNMP	Enable/Disable	Enable
	Read Community Name	Public
	Write Community Name	Private
	IP Address	0.0.0.0

3.2 System Requirements

Before configuration, please make sure your system meets the following requirements:

- A computer coupled with 10/ 100 Base-TX adapter;
- Configure the computer with a static IP address of 192.168.1.x, as the default IP address of EKI-

6311GN is 192.168.1.1. (X cannot be 0, 1, nor 255);

- A Web browser on PC for configuration such as Microsoft Internet Explorer 6.0 or above, Netscape or Firefox.

3.3 How to Login the Web-based Interface

The EKI-6311GN provides you with user-friendly Web-based management tool.

- Open Web browser and enter the IP address (Default: **192.168.1.1**) of EKI-6311GN into the address field. You will see the login page as below.



Figure 10 Login Page

- Enter the username (Default: **admin**) and password (Default: **password**) respectively and click "**Login**" to login the main page of EKI-6311GN. As you can see, this management interface provides five main options in the black bar above, which are Status, System, Wireless, Management and Tools.



Figure 11 Main Page

Note:

- The username and password are case-sensitive, and the password should be no more than 19 characters!

3.4 Basic System Settings

For users who use the EKI-6311GN for the first time, it is recommended that you begin configuration from "**Basic Settings**" in "**System**" shown below:



Figure 12 Basic System Settings

- **Basic Settings**

  Network Mode: Specify the network mode, including Bridge and Router. It is easy to configure parameters in Bridge Mode; however, users must pay extra attention to the way they configure the device when it is set to Router Mode. For details, please refer to **"IP Settings (Router)"**.
  Device Name: Specify the device name, which is composed of no more than 15 characters with (0-9), (A-Z), (a-z) or (-).
  Country Region: The availability of some specific channels and/or operational frequency bands is country dependent.

- **IP Settings (Bridge)**

  This is available only under Bridge network mode. Open "**IP Settings (Bridge)**" in "**System**" as below to configure the parameters for LAN which connects to the LAN port of EKI-6311GN. In this page, users may change the settings for IP Address, Subnet Mask, and DHCP Server.

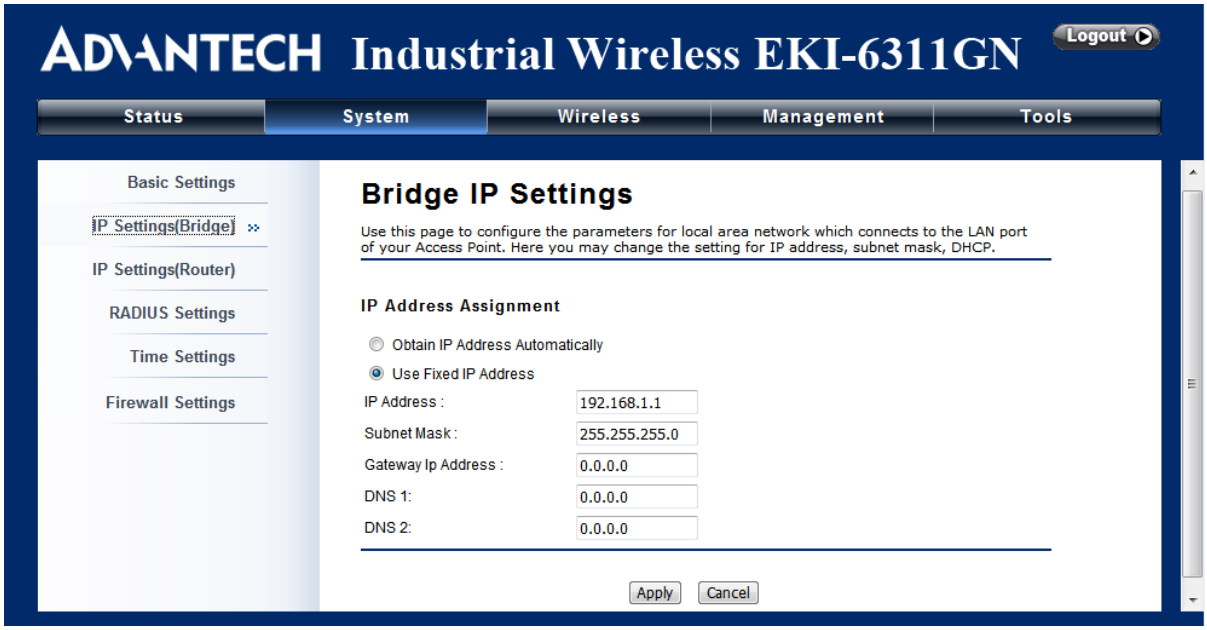


Figure 15 IP Settings (Bridge)

Obtain IP Address Automatically: If a DHCP server exists in your network, you can check this option, thus the EKI-6311GN is able to obtain IP settings automatically from that DHCP server.
Use Fixed IP Address: Check this option. You have to specify a static IP address, subnet mask, default gateway and DNS server for EKI-6311GN manually. Make sure the specified IP address is unique on your network in order to prevent IP conflict.
Spanning Tree: Spanning Tree Protocol (STP) is a link management protocol for AP which provides path redundancy while preventing loops in a network. STP allows only one active path at a time between the access points but establish the redundant link as a backup if the initial link fails.

- **IP Settings (Router)**

  This is available only under Router mode. Open "**IP Settings (Router)**" in "**System**" below to configure the parameters of EKI-6311GN for accessing the Internet.

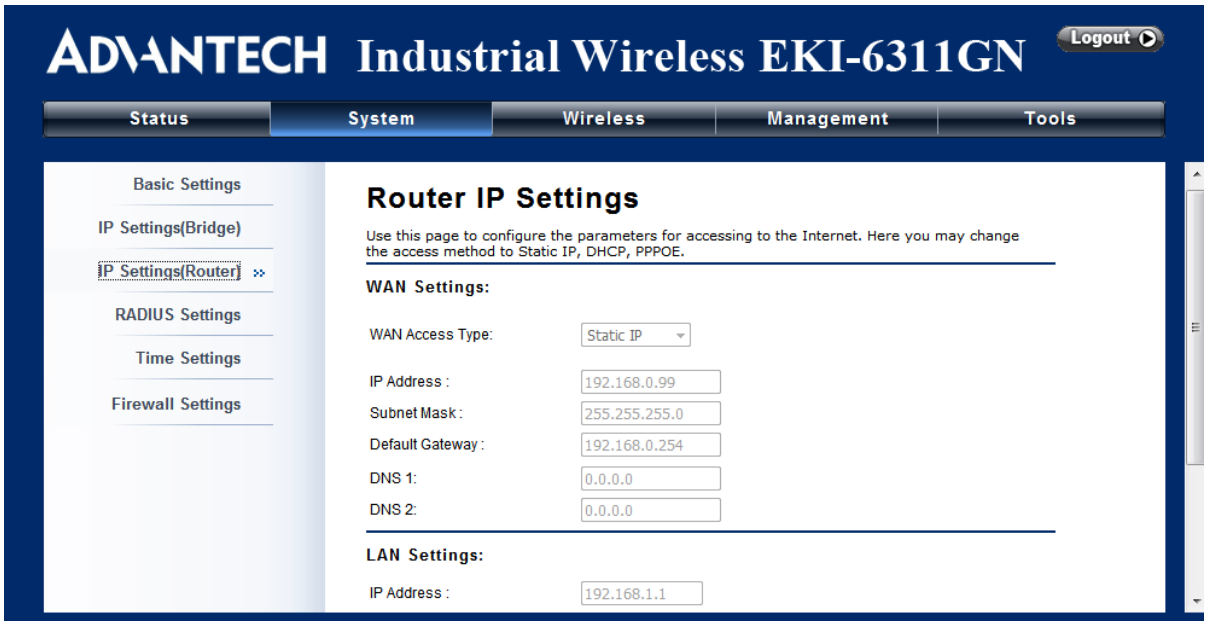


Figure 16 IP Settings (Router)

WAN Settings: Specify the Internet access method to Static IP, DHCP or PPPOE. Users must enter WAN IP Address, Subnet Mask, Gateway settings provided by your ISPs.

LAN Settings: When DHCP Server is disabled, users can specify IP address and subnet mask for EKI-6311GN manually. Make sure the specified IP address is unique on your network in order to prevent IP conflict. When DHCP Server is enabled, users may specify DHCP IP Address Range, DHCP Subnet Mask, DHCP Gateway and Lease Time (15-44640 minutes).

Warning:

- In AP mode, EKI-6311GN must establish connection with another wireless device before it is set to Router mode. In Router mode, it is impossible for users to access device via wired port, for WAN is on wired port and LAN is on wireless port. Users can access device through the wireless device connected with EKI-6311GN.
- In CPE mode, users can access EKI-6311GN via its wired port, for WAN is on wireless port and LAN is on wired port when device is set to Router mode.
- Bridge mode and AP Repeater mode are similar to AP mode when device is set to Router mode; WAN is on wired port and LAN is on wireless port. Thus users must also connect EKI-6311GN with another wireless device before it is set to Router mode and access EKI-6311GN via the connected wireless device.

3.5 RADIUS Settings

RADIUS (Remote Authentication Dial-In User Service) is a server for remote user authentication and accounting; playing a central role in the network in providing the capabilities of authenticating, authorizing, accounting, auditing, alarming and etc. It allows an organization to maintain user profiles in a central database that all remote servers can share.

Open “**RADIUS Settings**” in “**System**” to make RADIUS configuration.

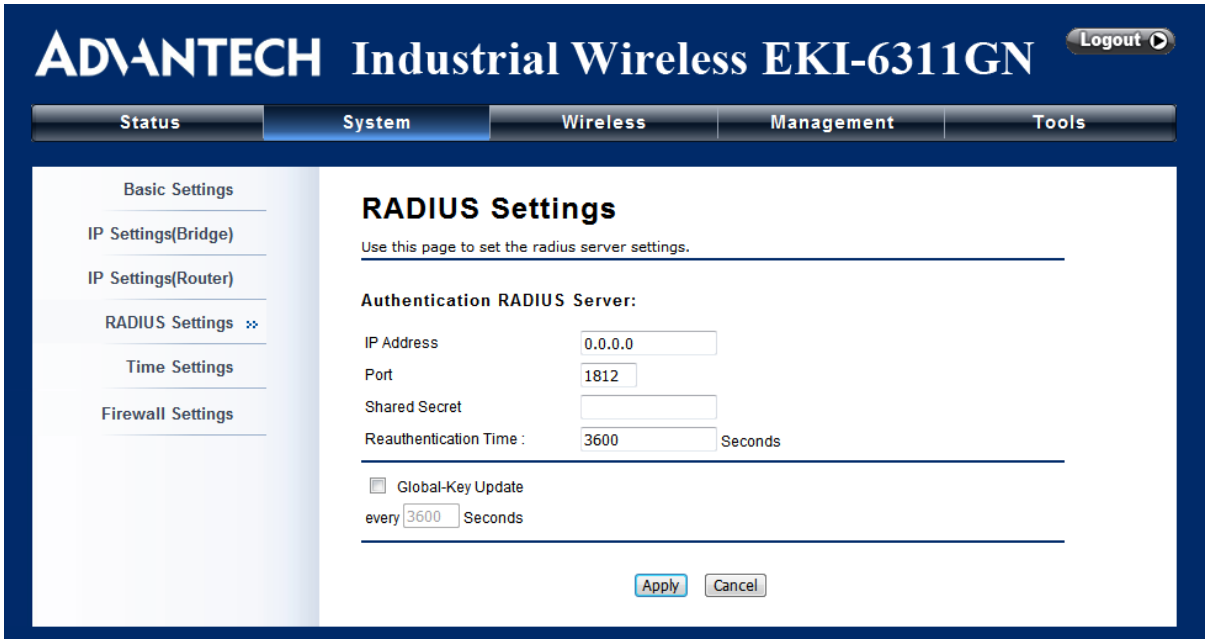


Figure 1713 RADIUS Settings

- **Authentication RADIUS Server**

  This is for RADIUS authentication. It can communicate with RADIUS through IP Address, Port and Shared Secret.

  IP Address: Enter the IP address of the Radius Server;

  Port: Enter the port number of the Radius Server;

  Shared Secret: This secret, which is composed of no more than 31 characters, is shared by the EKI-6311GN and RADIUS during authentication.

  Re-authentication Time: Set the time interval between two authentications.

  Global-Key Update: Check this option and specify the time interval between two global-key updates.

3.6 Time Settings

Compliant with NTP, the EKI-6311GN is capable of keeping its time in complete accord with the Internet time. Make configuration in “**Time Settings**” from “**System**”. To use this feature, check “**Enable NTP Client Update**” in advance.



Figure 18 Time Settings

- **Current Time**

  Display the present time in Yr, Mon, Day, Hr, Min and Sec.A

- **Time Zone Select**

  Select the time zone from the dropdown list.

- **NTP Server**

  Select the time server from the "**NTP Server**" dropdown list or manually input the IP address of available time server into "**Manual IP**".
  Hit "**Apply**" to save settings.

3.7 Firewall Settings

The firewall is a system or group of systems that enforce an access control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an un-trusted network. EKI-6311GN has capabilities of Source IP Filtering, Destination IP Filtering, Source Port Filtering, Destination Port Filtering, Port Forwarding as well as DMZ. This is available only under Router Mode.

Source IP Filtering: The source IP filtering gives users the ability to restrict certain types of data packets from your local network to Internet through EKI-6311GN. Use of such filters can be helpful in securing or restricting your local network.



Figure 19 Source IP Filtering

Destination IP Filtering: The destination IP filtering gives you the ability to restrict the computers in LAN from accessing certain websites in WAN according to specified IP addresses. Check the "**Enable Source IP Filtering**" checkbox and enter the IP address of the clients to be restricted. Hit **Apply** to make the setting take effect.



Figure 20 Destination IP Filtering

Source Port Filtering: The source port filtering enable you to restrict certain ports of data packets from your local network to Internet through EKI-6311GN. Use of such filters can be helpful in securing or restricting your local network.



Figure 21 Source Port Filtering

Destination Port Filtering: The destination port filtering enables you to restrict certain ports of data packets from your local network to Internet through EKI-6311GN. Use of such filters can be helpful in securing or restricting your local network.



Figure 22 Destination Port Filtering

Port Forwarding: The port forwarding allows you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings ne are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind EKI-6311GN's NAT firewall.

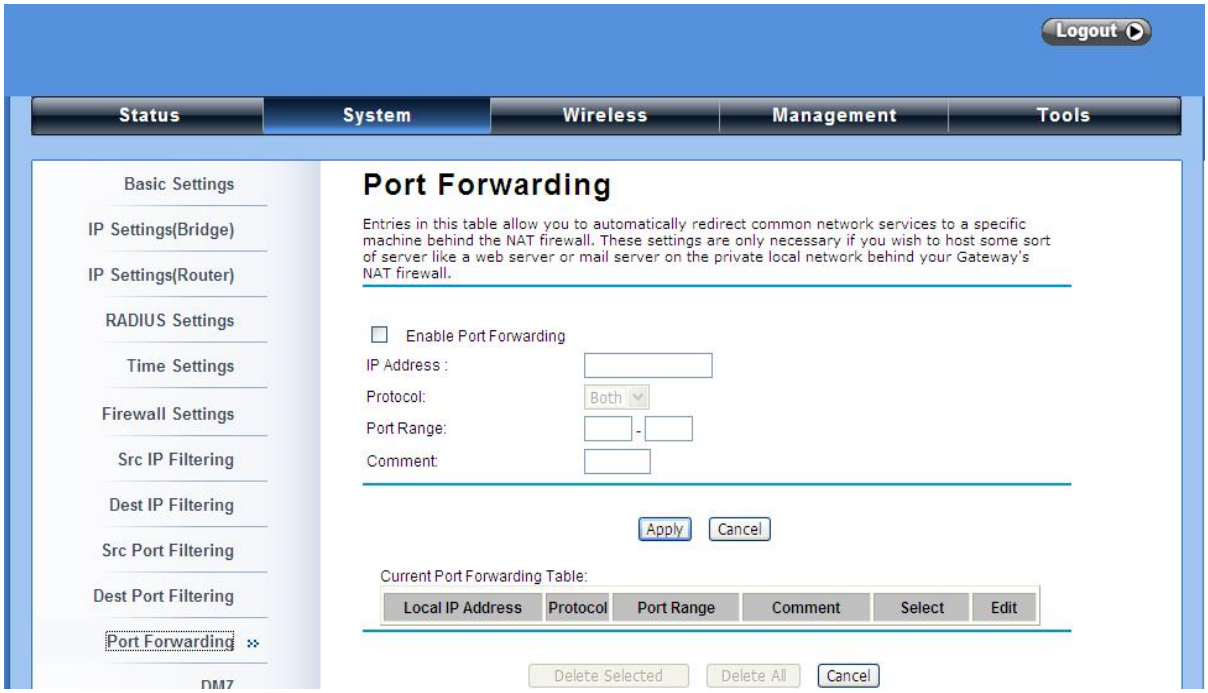


Figure 23 Port Forwarding

3.8 Basic Wireless Settings

Open "**Basic Settings**" in "**Wireless**" as below to make basic wireless configuration.



Figure 14 Basic Wireless Settings

- **Disable Wireless LAN Interface**

  Check this option to disable WLAN interface, then the wireless module of EKI-6311GN will stop working and no wireless device can connect to it.

- **Wireless Mode**

  Four operating modes are available on EKI-6311GN.
  Wireless Client: The EKI-6311GN is able to connect to the AP and thus join the wireless network around it.
  AP: The EKI-6311GN establishes a wireless coverage and receives connectivity from other wireless devices.
  Bridge: The EKI-6311GN establishes wireless connectivity with other APs by keying in remote MAC address. Please refer to the "WDS Setting" for detailed configuration.
  AP Repeater: The EKI-6311GN servers as AP and Bridge concurrently. In other words, the EKI-6311GN can provide connectivity services for CPEs under WDS mode.

- **Wireless Network Name (SSID)**

  This wireless network name is shared among all associated devices in your wireless network. Keep it identical on all those devices. Note that the SSID is case-sensitive and can not exceed 32 characters.

- **Broadcast SSID**

  Under AP mode, hiding network name is necessary when you are in a wireless environment that may have potential risk. By disabling broadcast SSID, the STA can not scan and find EKI-6311GN, so that malicious attack by some illegal STA could be avoided.

- **802.11 Mode**

  The EKI-6311GN can communicate with wireless devices of 802.11b/g or 802.11b/g/n. You can also select Auto and make it work under an appropriate wireless mode automatically.

- **HT Protect**

  Enable HT (High Throughput) protect to ensure HT transmission with MAC mechanism. Under 802.11n mode, wireless client can be divided into HT STA and Non-HT STA, among which the one with HT protect enabled gets higher throughput.

- **Channel Number**

  Channel varies much as the available band differs from country to country. Select a proper operating channel in the drop-down list according to your situation.

- **Antenna**

  By default, EKI-6311GN uses its built-in antenna for directional transmission; however, if you prefer to use an external antenna for your case-dependent applications, you can switch from "Internal (8 dBi)" to"External (N-Type)".

Note:

- You are able to choose "External (N-Type)" only when you have well done installing the external antenna; otherwise, it might damage EKI-6311GN itself.

- **Output Power**

  Specify the signal transmission power. The higher the output power is, the wider the signal can cover, but the power consumption will be greater accordingly. Usually "**Full**" is preferred.

- **Data Rate**

Usually “**Auto**” is preferred. Under this rate, the EKI-6311GN will automatically select the highest available rate to transmit. In some cases, however, like where there is no great demand for speed, you can have a relatively-low transmit rate for compromise of a long distance.

- **Channel Mode**

  Four levels are available: 5MHz, 10MHz, 20MHz and 40MHz. The last one can enhance data throughput, but it takes more bandwidth, thus it might cause potential interference.

- **Extension Channel Protection Mode**

  This is to avoid conflict with other wireless network and boost the ability of your device to catch all 802.11g transmissions. However, it may decrease wireless network performance. Compared to CTS-Self; the transmission amount of CTS-RTS is much lower.

- **Enable MAC Clone**

  Available only under wireless client mode, it hides the MAC address of the AP while displays the one of associated wireless client or the MAC address designated manually.

3.9 Site Survey

Under wireless client mode, the EKI-6311GN is able to perform site survey, through which, information on the available access points will be detected.
Open “**Basic Settings**” in “**Wireless**”, by clicking the “**Site Survey**” button beside “**Wireless Mode**” option, the wireless site survey window will popup with a list of available wireless networks around. Select the AP you would like to connect and click “**Selected**” to establish connection. The wireless site survey window can also be viewed by opening the “**Site Survey**” page in “**Tools**”.

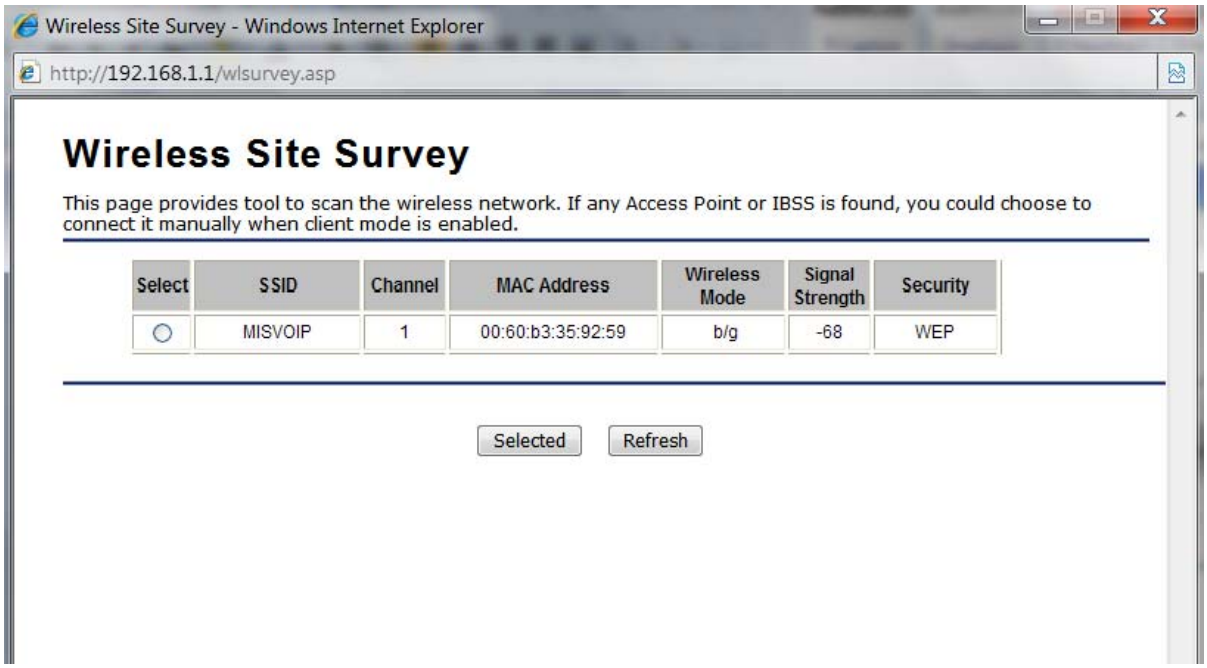


Figure 15 Site Survey

CHAPTER 4

Advanced Settings

Chapter 4 Advanced Settings

4.1 Advanced Wireless Settings

Open "**Advanced Settings**" in "**Wireless**" to make advanced wireless settings.



Figure 16 Advanced Wireless Settings

- **WMM Support**

  WMM (Wi-Fi Multimedia) is a subset of 802.11e. It allows wireless communication to define a priority limit on the basis of data type under AP mode only, thus those time-sensitive data, like video/audio data, may own a higher priority than common one. To enable WMM, the wireless client should also support it.

- **A-MPDU/A-MSDU Aggregation**

  The data rate of your AP except wireless client mode, could be enhanced greatly with this option enabled; however, if your wireless clients don't support A-MPDU/A-MSDU aggregation, it is not recommended to enable it.

- **Short GI**

  Under 802.11n mode, enable it to obtain better data rate if there is no negative compatibility issue.

- **RTS Threshold**

  The EKI-6311GN sends RTS (Request to Send) frames to certain receiving station and negotiates the sending of a data frame. After receiving an RTS, that STA responds with a CTS (Clear to Send) frame to acknowledge the right to start transmission. The setting range is 0 to 2346 in byte. Setting it too low may result in poor network performance. Leave it at its default of 2346 is recommended.

- **Fragmentation Length**

Specify the maximum size in byte for a packet before data is fragmented into multiple packets. Setting it too low may result in poor network performance. Leave it at its default of 2346 is recommended.

- **Beacon Interval**

  Specify the frequency interval to broadcast packets. Enter a value between 20 and 1024.

- **DTIM Interval**

  DTIM, which stands for Delivery Traffic Indication Message, is contained in the data packets. It is for enhancing the wireless transmission efficiency. The default is set to 1. Enter a value between 1 and 255.

- **Preamble Type**

  It defines some details on the 802.11 physical layer. "**Long**" and "**Short**" are available.

- **IGMP Snooping**

  IGMP snooping is the process of listening to IGMP network traffic. By enabling IGMP snooping, the AP will listen to IGMP membership reports, queries and leave messages to identify the ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group or groups.

- **Wireless Separation**

  Wireless separation is an ideal way to enhance the security of network transmission. Under the mode except wireless client mode, enable "**Wireless Separation**" can prevent the communication among associated wireless clients.

- **RIFS**

  RIFS (Reduced Inter-frame Spacing) is a means of reducing overhead and thereby increasing network efficiency.

- **Link Integration**

  Available under AP/Bridge/AP repeater mode, it monitors the connection on the Ethernet port by checking "**Enabled**". It can inform the associating wireless clients as soon as the disconnection occurs.

- **Max. Station Num**

  Available only under AP mode, it defines the maximum amount of wireless clients allowed to be connected.

- **Space in Meter/ACK Timeout**

  To decrease the chances of data retransmission at long distance, the EKI-6311GN can automatically adjust proper ACK timeout value by specifying distance of the two nodes.

- **Flow Control**

  It allows the administrator to specify the incoming and outgoing traffic limit by checking "**Enable Traffic Shaping**". This is only available in Router mode.

Note:

- We strongly recommend you leave most advanced settings at their defaults except "Distance in Meters" adjusted the parameter for real distance; any modification on them may negatively impact the performance of your wireless network.

4.2 Wireless Security Settings

To prevent unauthorized radios from accessing data transmitting over the connectivity, the EKI-6311GN provides you with rock solid security settings.

Security Settings

Open "**Security Settings**" in "**Wireless**" as below:



Figure 17 Security Settings

- **Network Authentication**
  - **Open System**: It allows any device to join the network without performing any security check.
  - **Shared Key**: Data encryption and key are required for wireless authentication.
  - **Legacy 802.1x**: As an IEEE standard for port-based Network Access Control, it provides the rights to access the wireless network and wired Ethernet. With User and PC identity, centralized authentication as well as dynamic key management, it controls the security risk of wireless network to the lowest. To serve the 802.1x, at least one EAP type should be supported by the RADIUS Server, AP and wireless client.
  - **WPA with RADIUS**: With warrant (username, password and etc.) offered by user, this kind of authentication can be realized with specific RADIUS server. This is the common way to be adopted in large enterprise network.
  - **WPA2 with RADIUS**: As a new version of WPA, only all the clients support WPA2, can it be available. If it is selected, AES encryption and RADIUS server is required.
  - **WPA&WPA2 with RADIUS**: It provides options of WPA (TKIP) or WPA2 (AES) for the client. If it is selected, the data encryption type must be TKIP + AES and the RADIUS server must be set.
  - **WPA-PSK**: It is a simplified WPA mode with no need for specific authentication server. In this so-called WPA Pre-Shared Key, all you have to do is just pre-enter a key in each WLAN node and this is the common way to be adopted in large and middle enterprise as well as residential network.

- **WPA2-PSK**: As a new version of WPA, only all the clients support WPA2, can it be available. If it is selected, the data encryption can only be AES and the passphrase is required.
- **WPA-PSK&WPA2-PSK**: It provides options of WPA (TKIP) or WPA2 (AES) encryption for the client. If it is selected, the data encryption can only be TKIP + AES and the passphrase is required.

- **Data Encryption**

  If data encryption is enabled, the key is required and only sharing the same key with other wireless devices can the communication be established.
  - **None**: Available only when the authentication type is open system.
  - **64 bits WEP**: It is made up of 10 hexadecimal numbers.
  - **128 bits WEP**: It is made up of 26 hexadecimal numbers.
  - **152 bits WEP**: It is made up of 32 hexadecimal numbers.
  - **TKIP**: Temporal Key Integrity Protocol, which is a kind of dynamic encryption, is co-used with WPA-PSK, etc.
  - **AES**: Advanced Encryption Standard, it is usually co-used with WPA2-PSK, WPA, WPA2, etc.
  - **TKIP + AES**: It allows for backwards compatibility with devices using TKIP.

Note:

- We strongly recommend you enable wireless security on your network!
- Only setting the same Authentication, Data Encryption and Key in the EKI-6311GN and other associated wireless devices, can the communication be established!

4.3 Access Control

The Access Control appoints the authority to wireless client on accessing EKI-6311GN, thus a further security mechanism is provided. This function is available only under AP mode.
Open "**Access Control**" in "**Wireless**" as below.



Figure 18 Access Control

- **Access Control Mode**

  If you select "**Allow Listed**", only those clients whose wireless MAC addresses are in the access control list will be able to connect to your AP. While when "**Deny Listed**" is selected, those wireless clients on the list will not be able to connect the AP.

- **MAC Address**

  Enter the MAC address of the wireless client that you would like to list into the access control list, click "**Apply**" then it will be added into the table at the bottom.

- **Delete Selected/All**

  Check the box before one or more MAC addresses of wireless client(s) that you would like to cancel, and click "**Delete Selected**" or "**Delete All**" to cancel that access control rule.

4.4 WDS Settings

Extend the range of your network without having to use cables to link the Access Points by using the Wireless Distribution System (WDS): Simply put, you can link the Access Points wirelessly. Open "**WDS Settings**" in "**Wireless**" as below:



Figure 30 WDS Settings

Enter the MAC address of another AP you wirelessly want to connect to into the appropriate field and click "**Apply**" to save settings.

Note:

- WDS Settings is available only under Bridge and AP Repeater Mode.

CHAPTER 5

Management

Chapter 5 Management

5.1 SNMP Management

The EKI-6311GN supports SNMP for convenient remote management. Open "**SNMP Configuration**" in "**Management**" shown below. Set the SNMP parameters and obtain MIB file before remote management.

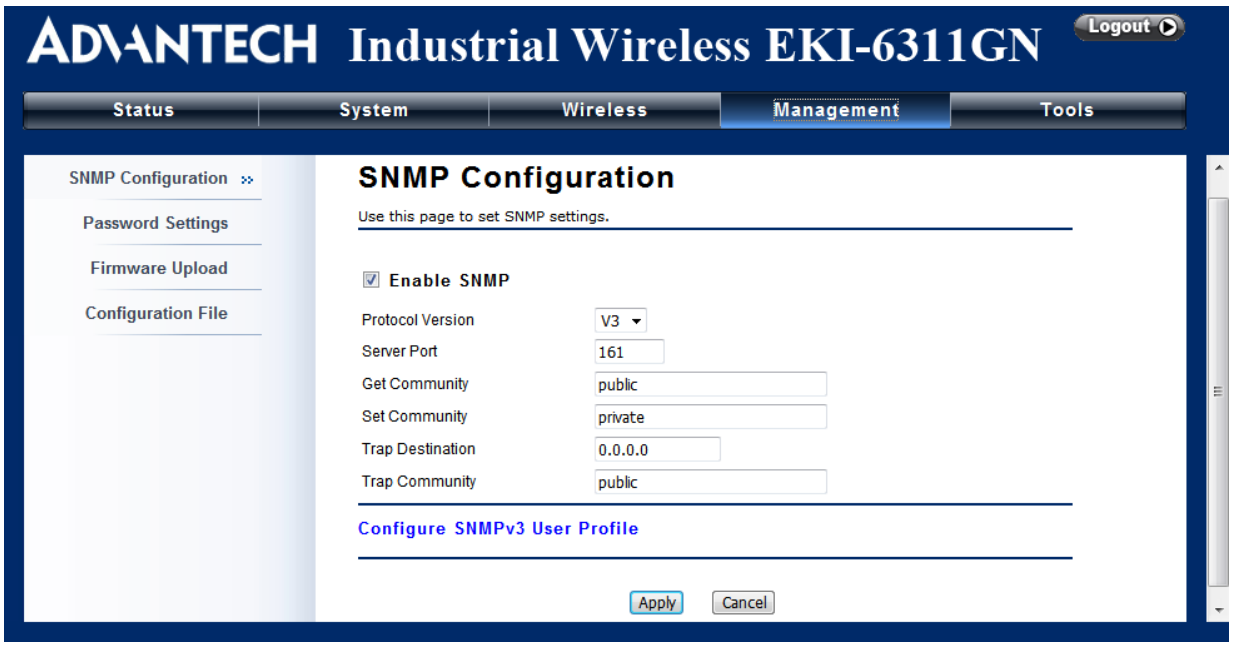


Figure 31 SNMP Configuration

- **Enable SNMP**

  Check this box to enable SNMP settings.

- **Protocol Version**

  Select the SNMP version, and keep it identical on the EKI-6311GN and the SNMP manager.

- **Server Port**

  Change the server port for a service if needed; however you have to use the same port to use that service for remote management.

- **Get Community**

  Specify the password for the incoming Get and GetNext requests from the management station. By default, it is set to public and allows all requests.

- **Set Community**

  Specify the password for the incoming Set requests from the management station. By default, it is set to private.

- **Trap Destination**

  Specify the IP address of the station to send the SNMP traps to.

- **Trap Community**

Specify the password sent with each trap to the manager. By default, it is set to public and allows all requests.

Configure SNMPv3 User Profile

For SNMP protocol version 3, you can click "**Configure SNMPv3 User Profile**" in blue to set the details of SNMPv3 user. Check "**Enable SNMPv3 Admin/User**" in advance and make further configuration.



Figure 32 Configure SNMPv3 User Profile

- **User Name**

  Specify a user name for the SNMPv3 administrator or user. Only the SNMP commands carrying this user name are allowed to access the EKI-6311GN.

- **Password**

  Specify a password for the SNMPv3 administrator or user. Only the SNMP commands carrying this password are allowed to access the EKI-6311GN.

- **Confirm Password**

  Input that password again to make sure it is your desired one.

- **Access Type**

  Select "**Read Only**" or "**Read and Write**" accordingly.

- **Authentication Protocol**

  Select an authentication algorithm. SHA authentication is stronger than MD5 but is slower.

- **Privacy Protocol**

  Specify the encryption method for SNMP communication. None and DES are available.
  None: No encryption is applied.
  DES: Data Encryption Standard, it applies a 58-bit key to each 64-bit block of data.

5.2 Password

From “**Password Settings**” in “**Management**”, you can change the password to manage your EKI-6311GN.

Enter the new password respectively in “**New Password**” and “**Confirm Password**” fields; click “**Apply**” to save settings.



Figure 33 Password

Note:

- The password is case-sensitive and its length can not be exceed 19 characters!

Upgrade Firmware

Open “**Firmware Upload**” in “**Management**” and follow the steps below to upgrade firmware locally or remotely through EKI-6311GN’s Web:



Figure 34 Upgrade Firmware

- Click “**Browse**” to select the firmware file you would like to load;
- Click “**Upload**” to start the upload process;
- Wait a moment, the system will reboot after successful upgrade.

Note:

- Do NOT cut the power off during upgrade, otherwise the system may crash!

5.3 Backup/ Retrieve Settings

It is strongly recommended you back up configuration information in case of something unexpected. If tragedy hits your device, you may have an access to restore the important files by the backup. All these can be done by the local or remote computer.

Open "**Configuration File**" in "**Management**" as below:



Figure 35 Backup/Retrieve Settings

- **Backup Settings**

  By clicking "**Save**", a dialog box will pop up. Save it, then the configuration file like **ap.cfg** will be saved to your local computer.

- **Retrieve Settings**

  By clicking "**Browse**", a file selection menu will appear, select the file you want to load, like **ap.cfg**; Click "**Upload**" to load the file. After automatically rebooting, new settings are applied.

5.4 Restore Factory Default Settings

The EKI-6311GN provides two ways to restore the factory default settings:

- **Restore factory default settings via Web**

  From "**Configuration File**", clicking "**Reset**" will eliminate all current settings and reboot your device, then default settings are applied.

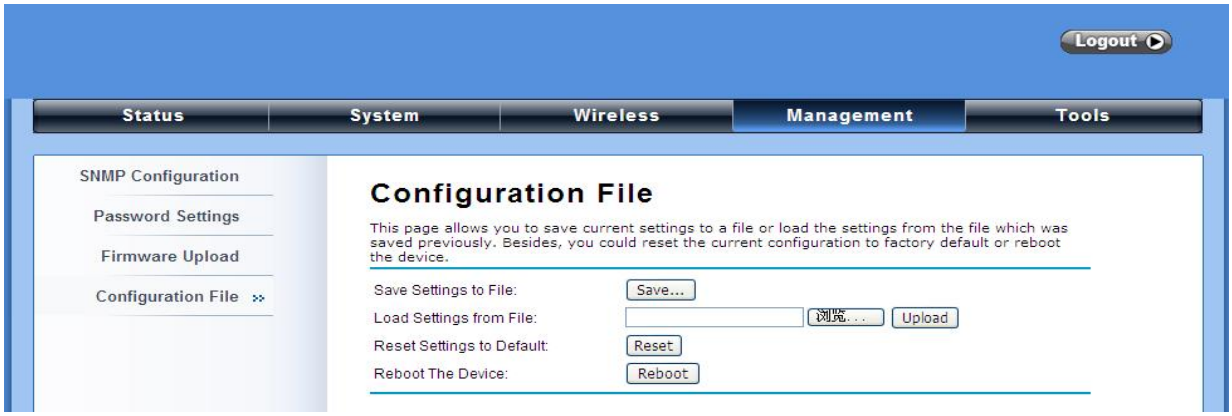


Figure 19 Restore Settings

- **Restore factory default settings via RS-232**

  If software in EKI-6311GN is unexpectedly crashed and no longer reset the unit via Web, you may do hardware reset via the reset button.

5.5 Reboot

You can reboot your EKI-6311GN from "**Configuration File**" in "**Management**" as below:
Click "**Reboot**" and hit "**Yes**" upon the appeared prompt to start reboot process. This takes a few minutes.

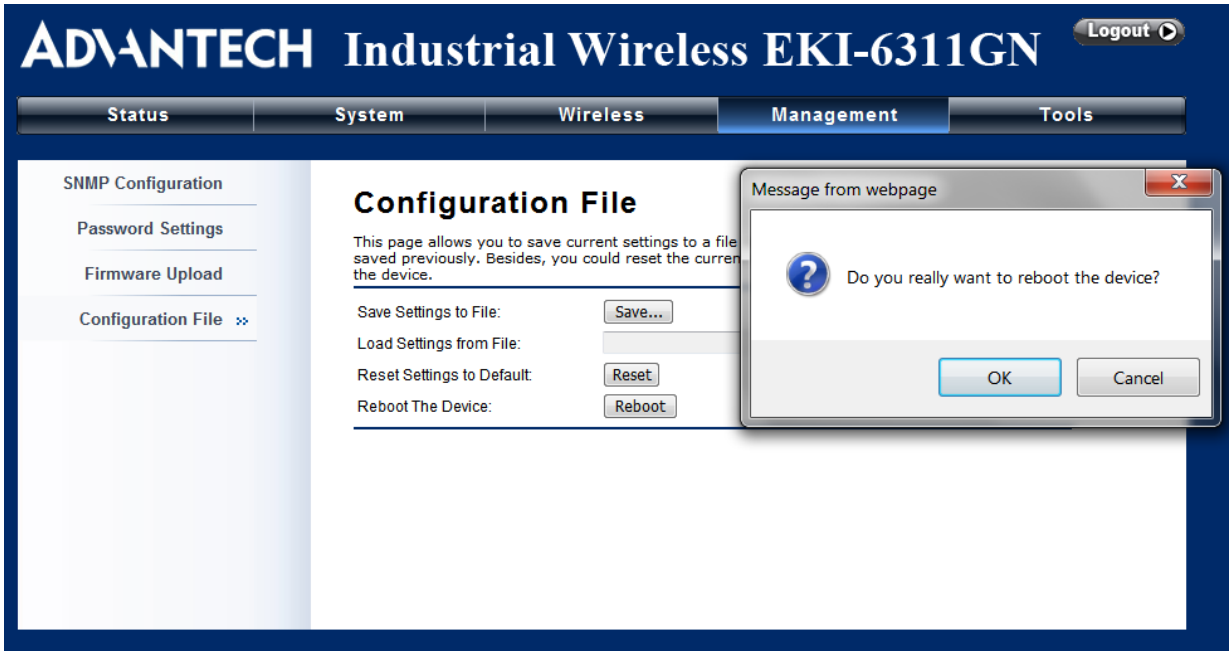


Figure 37 Reboot

5.6 System Log

System log is used for recording events occurred on the EKI-6311GN, including station connection, disconnection, system reboot and etc.
Open "**System Log**" in "**Tools**" as below.



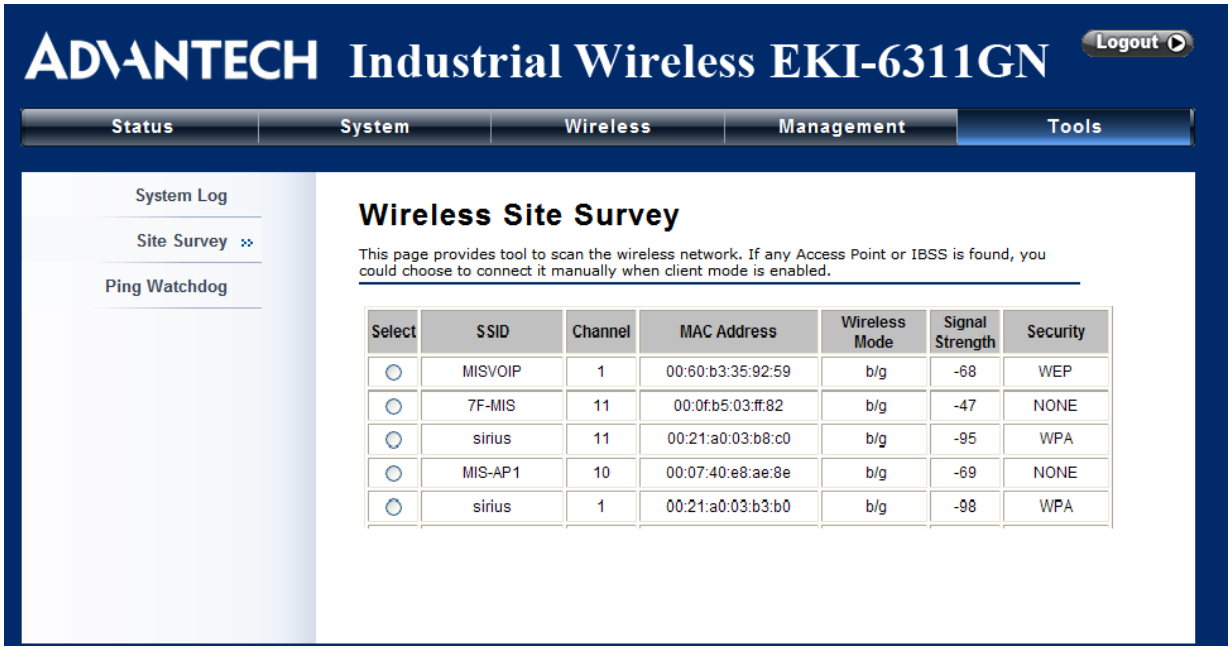
Figure 38 System Log

- **Remote Syslog Server**

  Enable Remote Syslog: Enable System log to alert remote server.
  IP Address: Specify the IP address of the remote server.
  Port: Specify the port number of the remote server.

5.7 Site Survey

Only available under Wireless Client mode, site survey allows you to scan all the APs within coverage.



5.8 Ping Watch Dog

If you mess your connection up and cut off your ability the log in to the unit, the ping watchdog has a chance to reboot due to loss of connectivity.



- **Ping Watchdog**

  Enable Ping Watchdog: To activate ping watchdog, check this checkbox.
  IP Address to Ping: Specify the IP address of the remote unit to ping.
  Ping Interval: Specify the interval time to ping the remote unit.
  Startup Delay: Specify the startup delay time to prevent reboot before the EKI-6311GN is fully initialized.
  Failure Count To Reboot: If the ping timeout packets reached the value, the ZCN-1523G-2-8 will reboot automatically.

CHAPTER 6

Status

Chapter 6 Status

6.1 View EKI-6311GN Basic Information

Open “**Information**” in “**Status**” to check the basic information of EKI-6311GN, which is read only. Click “**Refresh**” at the bottom to have the real-time information.



Figure 20 Basic Information

6.2 View Association List

Open “**Association List**” in “**Connection**” from “**Status**” to check the information of associated wireless clients. All is read only. Click “**Refresh**” at the bottom to view the current association list.



Figure 21 Connection

6.3 View Network Flow Statistics

Open “**Network Flow**” in “**Status**” to check the data packets received on and transmitted from the wireless and Ethernet ports. Click “**Refresh**” to view current statistics.

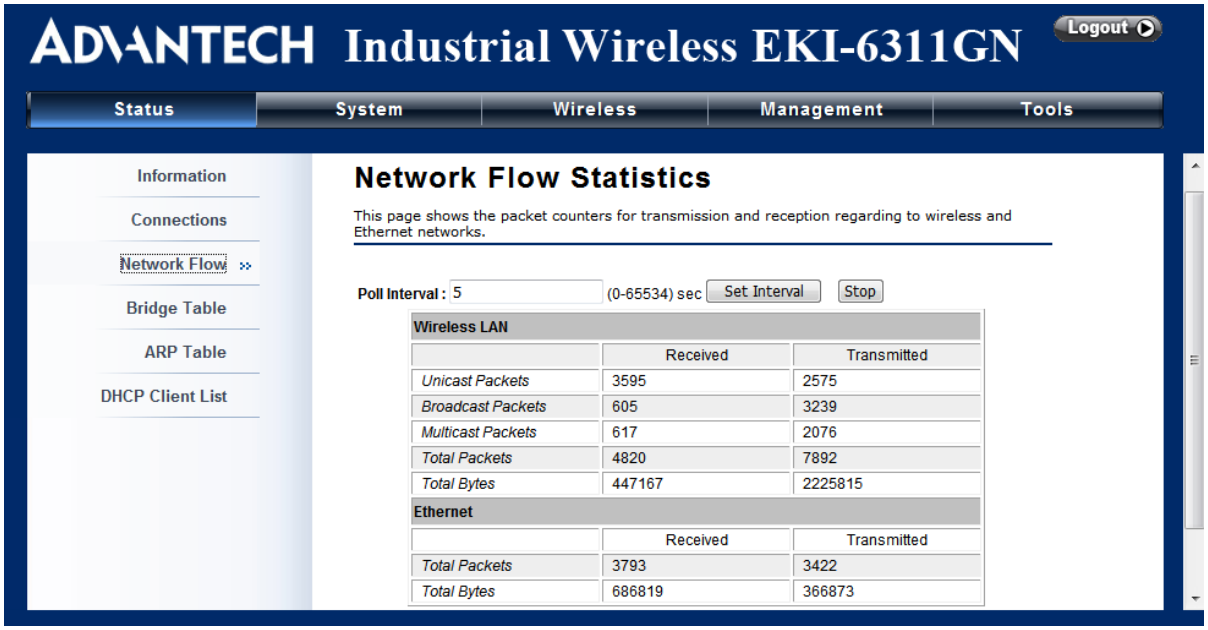


Figure 22 Network Flow Statistics

- **Poll Interval**

  Specify the refresh time interval in the box beside “**Poll Interval**” and click “**Set Interval**” to save settings. “**Stop**” helps to stop the auto refresh of network flow statistics.

6.4 View Bridge Table

Open “**Bridge Table**” in “**Status**” as below. Click “**Refresh**” to view current connected status..

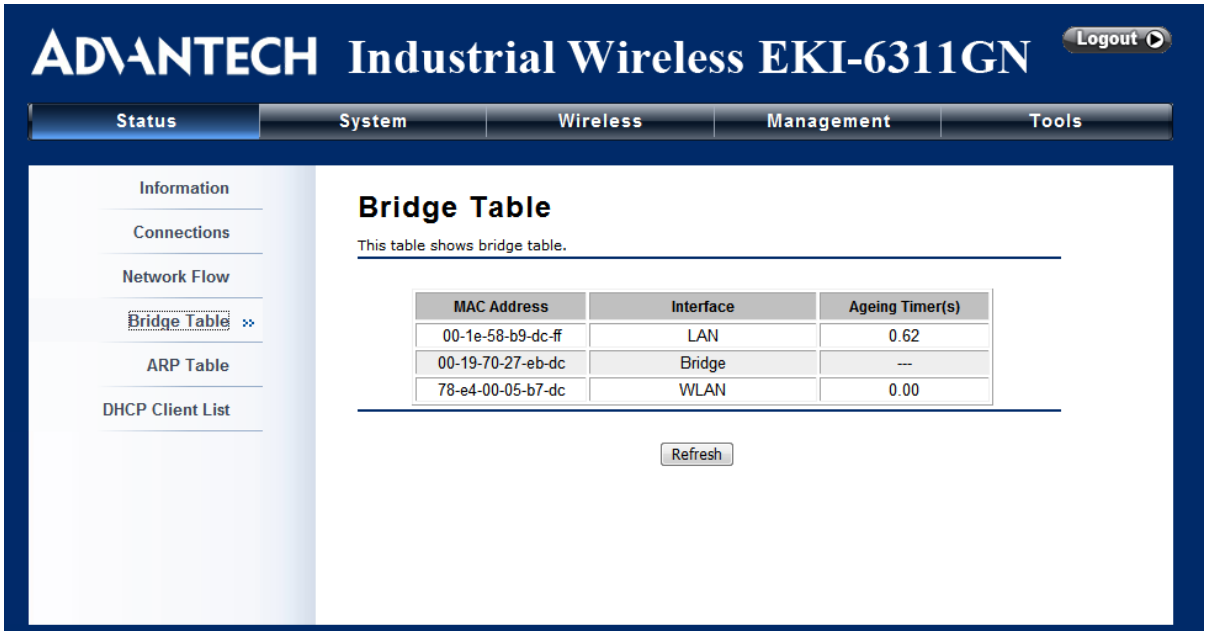


Figure 42 Bridge Table

6.5 View ARP Table

Open “**ARP Table**” in “**Status**” as below. Click “**Refresh**” to view current table.

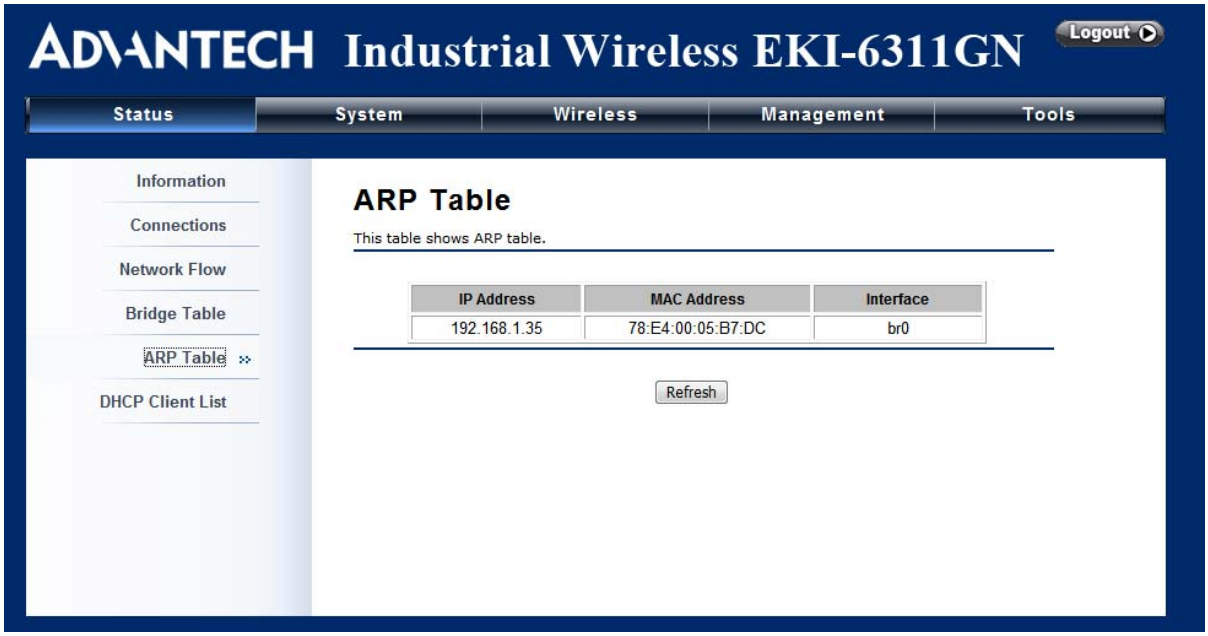


Figure 43 ARP Table

6.6 View Active DHCP Client Table

Open “**DHCP Client List**” in “**Status**” as below to check the assigned IP address, MAC address and time expired for each DHCP leased client. Click “**Refresh**” to view current table.



Figure 44 DHCP Client Table

CHAPTER 7

Trouble Shooting

Chapter 7 Trouble shooting

This chapter provides trouble shooting procedures for basic problems with the EKI-6311GN. For warranty assistance, contact your service provider or distributor for the process.

Q 1. How to know the MAC address of EKI-6311GN?

MAC Address distinguishes itself by the unique identity among network devices. There are two ways available to know it.

- Each device has a label posted with the MAC address. Please refer below.

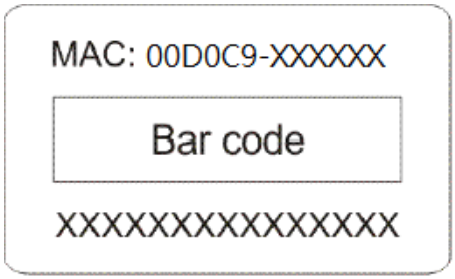


Figure 23 MAC Address

Q 2. What if I would like to reset the unit to default settings?

You may restore factory default settings in "**Configuration File**" from "**Management**".

Q 3. What if I would like to backup and retrieve my configuration settings?

You may do the backup by generating a configuration file or retrieve the settings you have backed up previously in "**Configuration File**" from "**Management**".

Q 4. What if I cannot access the Web-based management interface?

Please check the followings:

- Check whether the power supply is OK; Try to power on the unit again.
- Check whether the IP address of PC is correct (in the same network segment as the unit);
- Login the unit via other browsers such as Firefox.
- Hardware reset the unit.

Q 5. What if the wireless connection is not stable after associating with an AP under wireless client mode?

- Since the EKI-6311GN comes with a built-in directional antenna, it is recommended make the EKI-6311GN face to the direction where the AP is to get the best connection quality.
- In addition, you can start "**Site Survey**" in "**Wireless Basic Settings**" to check the signal

strength. If it is weak or unstable (The smaller the number is, the weaker the signal strength is.), please join other available AP for better connection.